OK AS TO FORM
A.M.H. 5.13.2020

Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

The Ohio State University

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and The Ohio State University on behalf of International Data Evaluation Center an instrumentality of the State of Ohio ("Services Provider") describes the services to be provided to JCPS by Services Provider, and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of **July 1 2020** and will terminate **June 23 2023** unless terminated earlier by either party pursuant to Section H.

B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following services to JCPS under the terms of a services contract between JCPS and Services Provider effective July 1 2020:

   The International Data Center (IDEC), http://www.idecweb.us, is department of the College of Education and Human Ecology at The Ohio State University (hereinafter referred to as OSU). IDEC is responsible for collecting data for Reading Recovery in the United States. Reading Recovery is a short-term intervention for first graders. IDEC uses the data to create reports and data dumps that can be used by Reading Recovery stakeholders to evaluate the effectiveness of their respective Reading Recovery programs. IDEC also publishes a national report annually and will conduct its own internal research to examine trends in Reading Recovery. This national report will not contain personally identifiable student information; it will contain aggregate data only.

2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, upon written request, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and

the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

3. JCPS shall disclose to Services Provider, upon written request, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3, under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The confidential data including student and non-student information to be disclosed is described in a document attached to this agreement as **Attachment A.** Services Provider shall use personally identifiable information from education records and other records in order to perform the services described in Paragraph B.1 above. Services Provider shall notify JCPS and JCPS shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the services or any changes to the scope, purpose or duration of the services themselves. Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the services contract described in Paragraph B.1 above.

4. Services Provider and JCPS shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. Services Provider shall confirm the transfer of confidential data and notify JCPS as soon as practicable of any discrepancies between the actual data transferred and the data described in this Agreement. The same protocol shall apply to any transfer of confidential data from Services Provider to JCPS.

C. CONSTRAINTS ON USE OF DATA

1. Services Provider agrees that the services shall be provided in a manner that does not permit personal identification of parents and students by individuals other than representatives of Services Provider that have legitimate interests in the information.

2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS.

3. Services Provider shall not re-disclose any individual – level data with or without identifying information to any other requesting individuals, agencies, or organizations who are not listed on Service Providers IRB without prior written authorization by JCPS.

4. Services Provider shall use the data only for the purpose described in Paragraph B.1 above. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to comply with all applicable JCPS, Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any data regarding any JCPS student that is subject to FERPA, Services Provider agrees to:

   a. In all respects comply with the provisions of FERPA.

   b. Use any such data for no purpose other than to fulfill the purposes of the services contract described in Paragraph B.1 above, and not share any such data with any person or entity other than Services Provider and its employees, contractors and agents, as approved by Service Provider's IRB, without the prior written approval of JCPS.

   c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.

   d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data expect as necessary to fulfill the purposes of the services contract described in Paragraph B.1 above.

   e. Provide the services under the services contract described in Paragraph B.1 above in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agent of Services Provider having a legitimate interest in knowing such personal identification.

   f. Destroy or return to JCPS any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Services Provider for the purposes of the services contract described in Paragraph B.1 above.

3. Services Provider shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Services Provider becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall use all reasonable efforts to provide JCPS with prior notice before disclosure so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a

protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of confidential and otherwise personally identifiable data that Services Provider is legally required to disclose.

4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data.

5. Services Provider shall not use data shared under this Agreement for any purpose other than the services contract described in Paragraph B.1 above. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the data to Services Provider.

6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include, but are not limited to:

    a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;

    b. Encrypting all data carried on mobile computers/devices;

    c. Encrypting data before it is transmitted electronically;

    d. Requiring that users be uniquely identified and authenticated before accessing data;

    e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the data necessary for this to perform their job functions;

    f. Ensuring that all staff accessing data have been trained in proper data protection as outlined in Service Provider's policies and procedures manual, the relevant excerpt of which is attached as Attachment B.

    g. Securing access to any physical areas/electronic devices where sensitive data are stored;

    h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and

    i. Installing anti-virus software to protect the network.

7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information by,

without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

a. "Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

    i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

    ii. A Social Security number;

    iii. A taxpayer identification number that incorporates a Social Security number;

    iv. A driver's license number, state identification card number or other individual identification number issued by an agency;

    v. A passport number or other identification number issued by the United States government; or

    vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

b. As provided in KRS 61.931(5), a "non-affiliated third party" means "any person or entity that has a contract or agreement with the Commonwealth and receives (accesses, collects or maintains) personal information from the Commonwealth pursuant to the contract or agreement."

c. Services Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.

d. Services Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person or entity other than an educational institution that operates a cloud computing service"), Services Provider agrees that:

    a. Services Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Services Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

b. With a written agreement for educational research, Services Provider may assist an educational institution to conduct educational research as permitted by FERPA.

c. Pursuant to KRS 365.734, Services Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

d. Pursuant to KRS 365.734, Services Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

e. Pursuant to KRS 365.734, Services Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

9. Services Provider shall report all known or suspected breaches of the data, in any format, to Dr. Dena Dossett, Chief, Data Management, Planning and Program Evaluation Division. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discover the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, or a breach of hard copies of records; (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.

10. Services Provider shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, when no longer needed for the purposes for which the study was conducted. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the data has been destroyed.

11. For purposes of this agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates Jeff Brymer-Bashore, Director and Co-Principal investigator, (or an alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. JCPS or its agents may, upon request, review the records Services Provider is required to keep under this Agreement.

12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of protected student information constitutes just cause for JCPS to immediately terminate this Agreement.

E. FINANCIAL COSTS OF DATA-SHARING

Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student data requested under this agreement and costs associated with the electronic delivery of the student data to Services Provider.

No payments will be made under this Agreement by either party. Any payments to Services Provider will be made under services contract described in Paragraph B.1 above.

F. OBLIGATIONS OF JCPS

During the term of this Agreement, JCPS shall:

1. Prepare and deliver student demographic and academic data as defined in **Attachment A** – Data File Description. All items will be keyed to a “proxy” student identifier that is different from the official student ID. The link between the official and proxy IDs will not be disclosed by JCPS. No personally identifiable information will be provided to Services Provider.

2. After the initial data is provided for the requested student population, JCPS will not provide supplementary data for additional students.

3. Provide Data Stewardship training for data custodian.

G. RESERVED

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):

    a. By either party immediately in the event of a material breach of this Agreement by another party.

    b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.

2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, the confidential information shall be returned or destroyed within seven (7) days of the termination. If this Agreement terminates at the end of the term described in Section A, Services Provider shall return or destroy all confidential information when it is no longer needed for the study. Such return or destruction shall occur within seven (7) days after it is no longer needed for the study.

3. Destruction of the confidential information shall be accomplished by utilizing an approved methods of confidential destruction, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer or researcher. If new materials are developed during the term of the services contract described in Paragraph B.1 above , ownership and copyright of such will be governed by the terms of the services contract.

J. MODIFICATION

No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

K. QUALITY OF SERVICES

JCPS reserves the right to review Services Provider's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1. Failure of Services Provider to perform in a manner that meets or exceeds the quality standards for JCPS shall serve as grounds for termination of this Agreement.

L. BREACH OF DATA CONFIDENTIALITY

Services Provider acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to JCPS for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by Services Provider, JCPS, in addition to any other rights and remedies available to JCPS at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that Services Provider has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), JCPS may not allow Services Provider access to personally identifiable information from education records for at least five (5) years.

M. RESERVED

N. WAIVER

No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right or prevent a similar subsequent act from constituting a violation of this Agreement.

O. SEVERABILITY

If any part of this Agreement is held to be void, against public policy or illegal, the balance of this Agreement shall continue to be valid and binding.

P. NOTICES

Any notices or reports by one party to the other party under this Agreement shall be made in writing, to the address shown in the signature portions of this Agreement, or to such other address as may be designated in writing by one party to the other. Notices shall be effective when received if personally delivered, or three days after mailing if mailed.

Q. RELATIONSHIP OF PARTIES

JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

R. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Services Provider shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of JCPS, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

Michael Papadakis
Sr. Vice President for Business and Finance and CFO
The Ohio State University

On behalf of the International Data Evaluation Center
1100 Kinnear Rd
Rm 129
Columbus, OH 43212

BY: ______________________

Name: Michael Papadakis, Sr. Vice President For Business & Finance, and CFO The Ohio State University

Title: ______________________

Date: 6·2·2020

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: ______________________

Name: ______________________

Title: ______________________

Date: ______________________

Attachment A

CONFIDENTIAL INFORMATION TO BE DISCLOSED

Reading Recovery Student Data

1. *Student Name*

2. *Student ID Number (Optional)*

3. *School*

4. *Gender*

5. *Date of Birth*

6. *[Data point removed by agreement of the parties. Space kept for consistency in numbering]*
7. *Native Language*

8. *Race/Ethnicity*

9. *Disability Status*

10. *Scores on a diagnostic tool called the Observation Survey/Instrumento de Observacion which is administered in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year, along with the dates the tool was administered.*

11. *Scores on a diagnostic tool called Slosson Oral Reading test which is administered in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year. (Optional)*

12. *Classroom literacy performance as compared to peers in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year.*

13. *English Proficiency in the fall if the child is not a native English speaker*

14. *The date the child's intervention started and ended.*

15. *Whether or not the child successfully completed the intervention*

16. *Misc. comments about the child's intervention if their intervention was not successful.*

17. *The length of the child's intervention in weeks*

18. *The number of lessons a child received*

19. *The number of lessons the student missed*

20. *The number of lessons the teacher missed*

21. *Number of days student was absent from school*

22. *Special education referral status*

23. *Did the child receive special education services*

24. *What type of special education services did child receive*

25. *How often were special services received*

26. *Where were special education services rendered*

27. *Whether or not child was retained in first grade*

28. *Did child receive supplemental literacy services*

29. *Who delivered supplemental literacy services*

30. *Where were supplemental literacy services provided*

31. *How often did child receive supplemental literacy services*

32. *Did child receive remedial education services*

33. *When did child receive remedial education services*

34. *How often were remedial education services delivered*

35. *Did child receive ESL services*

36. *When did child receive ESL services*

37. *Did child receive bilingual or dual-language education services*

38. *What type of daily guided reading did child receive*

39. *When was bilingual or dual-language education initiated*

Teacher Data

1. *Reading Recovery Training Status*

2. *When did the teacher complete Reading Recovery Training*

3. *Number of years in Reading Recovery*

4. *Number of Reading Recovery students instructed per day*

5. *Teacher's other role in a school*

6. *Number of students instructed outside of Reading Recovery by grade level*

7. *Gender*

8. *Race/Ethnicity*

9. *Native Language*

10. *Number of years employed in education*

11. *Highest level of education*

School Data

1. *First and last day of school*

2. *Years of participation in Reading Recovery*

3. *Number of first graders enrolled in school*

4. *Number of first graders that need Reading Recovery*

5. *Sources of funding for Reading Recovery*

6. *Whether or not school has mandatory literacy assessment for first graders*

7. *List of literacy assessments used at school*

Attachment B

IDEC Data Access Security Policy

Purpose

This policy defines the proper procedures and precautions that must be taken by IDEC employees when accessing data to perform duties related to their jobs.

Definitions

1. Device – Any electronic device that can communicate with IDEC's computer systems via a network.
2. Local storage – a storage medium that is contained inside of a device used to store data. This includes, but not limited to, hard drives, solid state drives, and DVD/CD drives.
3. University Infrastructure – This refers to the network maintained by the Office of the Chief Information Officer at The Ohio State University
4. IDEC Data – This refers to data stored in IDEC's computer systems that contain personally identifiable or types of data the University considers sensitive.

Policies

1. Within reason, IDEC will provide all its employees the proper tools and training to access data in a secure manner.
2. IDEC acknowledges that student data continue to be the property of and under the control of local educational agencies.
3. IDEC will not use student data other than for the express purposes of conducting research and evaluation related to the Reading Recovery, Descubriendo la Lectura, and Literacy Lessons interventions.
4. IDEC will provide the proper equipment to employees to secure University owned devices used at remote locations.
5. No data shall ever be stored on a device that cannot have its internal storage encrypted.
6. IDEC employees may not use personal devices to access protected data.
7. IDEC employees will immediately report to the Director of IT and Operations the theft or loss of any equipment that has been accessing IDEC systems or may have contained IDEC data.
8. IDEC employees will immediately report to the Director of IT and Operations the theft or loss of any IDEC data.
9. IDEC will keep student's data for the length of the research project and delete all data once research is complete.

10. Any device accessing IDEC Data must be password protected and may not use any sort of auto-login feature.
11. Any device accessing IDEC systems must be capable of providing a screen-locking mechanism that requires the use of a password to unlock. It is a requirement that it be set to lock automatically after a period of 5 minutes.
12. IDEC employees must lock the screens of any device when leaving the device unattended for any period of time.
13. If IDEC data are to be transported on some type of removable media, the data must be stored in an encrypted format.

Data Center Security

Purpose

This section describes the measures that are taken to protect the computers running IDEC's data systems

Description

IDEC's data systems are stored at the College of Education and Human Ecology's data center located at the State of Ohio Data Center. Access to this building is controlled by two-factor authentication. To enter and move around inside the building one must have an access card to open a door. This includes the doors on the outside of building. Once a card is swiped, the person holding the card must enter a PIN number as the second part of the authentication process. If the PIN is incorrect, the door will not open. The servers that run our data systems are stored in a locked cage that can only be accessed using this 2-factor authentication of swiping a card and supplying a PIN number. A security guard is also present watching the front doors. Data systems are also protected from electronic intrusion by a network firewall. Our web sites use 256-bit SSL (Secure Sockets Layer) encryption to protect data as it is being entered by teachers.

Data Breach Mitigation Policy

Purpose

This section describes the actions that need to be taken in the event that data are stolen from IDEC. This policy does not cover the accidental release of data by an IDEC employee. Those should be handled on a case-by-case IDEC's Directors of IT and Operations. He / She will choose the appropriate course of action to handle the matter.

Description

The following actions will take place in the event of data breach

1. Notifications process
   a. Notify IDEC's Director

b. Notify Office Responsible Practices, done by Director
c. Notify Office of Information Technology for the College of Education
d. If appropriate, notify proper Authorities
e. Gather Description of Event
f. Identify Location of Event

2. Investigation Steps
   a. Establish a response team (Director of IT and Op; Systems Manager, Director)
   b. Identify and take immediate action to stop the source of the attack or entity responsible
   c. Determine and notify key stakeholder (ie TLs, Trainers, Principals, etc..). Director will determine who to notify with help of IDEC staff.
   d. Identify source or suspects of the event
   e. Carry out IT forensics investigation to gather evidence
   f. Determine need for external law enforcement
   g. Determine to contact other additional stakeholders
3. Other Actions if Applicable
   a. Contact law enforcement
   b. Collection of evidence
   c. Notification of victims
   d. Prepare written communication plan to cover oral and written communication to parties involved
   e. Communication with media
4. Follow-up activities
   a. Evaluation of Security Incident Response
   b. Determine
      i. How well did the work force members respond to event?
      ii. Were documented procedures followed? Were they adequate?
      iii. What information was needed sooner?
      iv. Were there any steps or actions that might have inhibited recovery?
      v. What could work force members do differently the next time an incident occurs?
      vi. What corrective actions can prevent similar events in the future?
      vii. What additional resources are needed to detect, analyze, and mitigate future incidents?
      viii. What external resources and contacts proved helpful?
      ix. Other conclusions or recommendations